

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

Claims 1 - 58 (Canceled)

59. (New) A data isolation system for software and data maintenance, back up and recovery for a computer wherein dynamic data files are identified and passed into at least one hidden partition on a hard disk of the computer, the passing being by one or more selected from the group consisting of: copying and redirection;

wherein the at least one hidden partition and its content is neither manageable nor accessible by the computer's operating system; and the dynamic data files in the hidden partition are not accessible by any software application on the computer.

60. (New) The system as claimed in claim 59, wherein the group further includes filtering and access control.

61. (New) The system as claimed in claim 59, wherein automatic back ups are made to the dynamic data files in the hidden partition whenever the dynamic data files are accessed and modified.

62. (New) The system as claimed in claim 59, wherein the dynamic data files include the computer's operating environment so that the computer's operating environment can be restored from the dynamic data files in the hidden partition.

63. (New) The system as claimed in claim 59, wherein the dynamic data files in the hidden partition include data up to the time of a failure of the computer's system.

64. (New) The system as claimed in claim 59, wherein compression is used for at least one file of the dynamic data files in the hidden partition.

65. (New) The system as claimed in claim 59, wherein encryption is used for at least one of the dynamic data files in the hidden partition.

66. (New) The system as claimed in claim 59, wherein prior to copying the dynamic data files into the hidden partition, all software installed on the computer, including a primary operating system for the computer, is segregated into at least one static routine and the dynamic data files, dynamic data files including system configuration files, and user data files; the segregation comprising categorization; all data sent from the primary operating system to the dynamic data files and all data sent from the dynamic data files to the primary operating system is passed to the dynamic data files in the hidden partition; and the segregating or categorizing of the data files of is by use of a data isolation technique that consists of one or more selected from the group consisting of:

- (a) automatic selection of commonly used software application of the operating system;
- (b) automatic selection of commonly used software application
- (c) selection of software application by a user of the computer; and
- (d) selection of files or file folders by the user.

67. (New) The system as claimed in claim 59, wherein the dynamic data files in the hidden partition are continuously updated and the original dynamic data files in a main partition of the hard disk are continuously updated; an additional I/O driver being placed between a file system I/O interface and a disk driver for access control, intercepting, filtering and re-directing data for the dynamic data files in the hidden partition, the additional I/O driver using an secondary operating system; the access

control, intercepting, filtering and re-directing is by the use of regulatory, matching, and fulfillment tables; the additional I/O driver is part of one or more selected from the group consisting of: the disk driver, the file system I/O interface, and the operating system; the secondary operating system is different to the primary operating system; and back up and recovery use one of the primary operating system and the secondary operating system.

68. (New) The system as claimed in claim 59, wherein on system recovery, a last back up system environment in the hidden partition, including the copied dynamic data files, is recovered; the dynamic data files in the hidden partition including all data up to an instant before the recovery process was invoked, and the system environment including the primary operating system and software.

69. (New) The system as claimed in claim 59, wherein upon new software being installed in the computer, the installation is delayed until a back up of the existing system environment to the hidden partition is completed and, after completion of the back up, the installation is resumed; and if system instability or failure is encountered after the installation or running of the new software, the computer system restores the previous operating environment from the back up.

70. (New) The system as claimed in claim 59, wherein upon a new device driver being installed in the computer, the installation is delayed until a back up of the existing system environment to the hidden partition is completed and, after completion of the back up, the installation is resumed and, if system instability or failure is encountered after the installation or running of the new device driver, the computer system restores the previous operating environment from the back up.

71. (New) The system as claimed in claim 59, wherein software application and its dynamic data files are copied to the hidden partition as independent modules.

72. (New) The system as claimed in claim 59, wherein the dynamic data files in the hidden partition work as active data files for a software application and are continuously updated.

73. (New) The system as claimed in claim 66, wherein for (a), (b) and (c), all dynamic data files belonging to the software application will be automatically segregated and stored to the hidden partition; and for (d), the selected files or all the dynamic data files belonging to the selected file folders will be automatically segregated and stored to the hidden partition.

74. (New) The system as claimed in claim 59, wherein the dynamic data files stored in the hidden partition are protected.

75. (New) The system as claimed in claim 59, wherein the dynamic data files stored in the hidden partition are used as active working files and are continuously updated; a plurality of back-up copies of each dynamic data file in the hidden partition being made in the hidden partition using a first-in-first-out sequence; and upon accessing and modifying an working data file, the plurality of back-ups are updated according to a pre-assigned back-up schedule.

76. (New) A system for managing access to a host computer by a remote computer wherein access by the remote computer is in accordance with a software security access policy in the host computer; wherein dynamic data files are identified and passed into a hidden partition on a hard disk of the host computer, the passing being

by one or more selected from the group consisting of: copying, redirection, filtering, and access control.

77. (New) The system as claimed in claim 76, wherein the software security access policy has a file access right and control mechanism; and the file access right and control mechanism is used to selectively provide protection to selected software application and their respective dynamic data files; the file access right and control mechanism of the host computer by the remote computer being controlled by the host computer and include:

- (a) selection of software application/programs;
- (b) selection of dynamic data files of the software application;
- (c) selection of configuration files;
- (d) selection of data file or folder; and
- (e) selection of the type of the operation to be performed by the remote computer.

78. (New) The system as claimed in claim 77, wherein the selected file, or files belonging to the selected folder, are automatically given the access right while any others will be denied access; the file access right and control mechanism of the host computer being pre-determined by a category of the remote host computer and different remote computers are given different access rights for different usage; all files including program, configuration and user data being automatically given the access right while all others are denied access.

79. (New) The system as claimed in claim 78, wherein the host computer has an additional I/O driver placed between a file system I/O interface and a disk driver for access control, intercepting, filtering and re-directing data for the dynamic data files, the additional I/O driver using an secondary operating system; the access control,

intercepting, filtering and re-directing being by the use of regulatory, matching, and fulfillment tables; and the additional I/O driver is part of one or more selected from the group consisting of: the disk driver, the file system I/O interface, and the primary operating system.

80. (New) The system as claimed in claim 79, wherein the secondary operating system is different to the primary operating system; back up and recovery use one of the primary operating system and the secondary operating system; and the remote access is through the secondary operating system.

81. (New) The system as claimed in claim 76, wherein the selected software application and their respective dynamic data files are identified and are located in at least one partition of the primary operating system of the host computer.

82. (New) The system as claimed in claim 76, wherein the host computer using diagnostic utilities to allow remote technical support by the remote computer.

83. (New) A system for providing an external back up for at least one computer to at least one hidden partition of a centralized back up server, wherein dynamic data files of the at least one computer are identified and passed into the at least one hidden partition on a hard disk of the centralized back up server, the passing being by one or more selected from the group consisting of: copying and redirection.

84. (New) The system as claimed in claim 83, wherein the at least one hidden partition of the centralized back up server is accessed using at least one selected from the group consisting of a: LAN, WAN, VPN, Intranet and Internet; critical applications and their dynamic data files being stored and protected in the at least one hidden partition of the centralized back up server by using encryption and are only able to be accessed by authorized users.

85. (New) The system as claimed in claim 84, wherein the at least one computer has an additional I/O driver placed between a file system I/O interface and a disk driver for access control, intercepting, filtering and re-directing data for the dynamic data files, the additional I/O driver using a secondary operating system; the access control, intercepting, filtering and re-directing being by the use of regulatory, matching, and fulfillment tables; the additional I/O driver being part of one or more selected from the group consisting of: the disk driver, the file system I/O interface, and the primary operating system.

86. (New) The system as claimed in 83, wherein the secondary operating system is different to a primary operating system of the at least one computer; back up and recovery being by use one of the primary operating system and the secondary operating system.

87. (New) The system as claimed in claim 85, wherein communication with the centralized back up server is through the secondary operating system.

88. (New) The system as claimed in claim 59 further comprising a system for managing access to a host computer by a remote computer wherein access by the remote computer is in accordance with a software security access policy in the host computer; wherein dynamic data files are identified and passed into a hidden partition

on a hard disk of the host computer, the passing being by one or more selected from the group consisting of: copying, redirection, filtering, and access control.

89. (New) The system as claimed in claim 59 further comprising a system for providing an external back up for at least one computer to at least one hidden partition of a centralized back up server, wherein dynamic data files of the at least one computer are identified and passed into the at least one hidden partition on a hard disk of the centralized back up server, the passing being by one or more selected from the group consisting of: copying and redirection.

90. (New) The system for management of access to a host computer by a remote computer as claimed in claim 76 further comprising a system for providing an external back up for at least one computer to at least one hidden partition of a centralized back up server, wherein dynamic data files of the at least one computer are identified and passed into the at least one hidden partition on a hard disk of the centralized back up server, the passing being by one or more selected from the group consisting of: copying and redirection.